North Dakota
Homeland Security
Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

Quick Links

North Dakota

Nothing Significant to Report

Regional

(Minnesota) **Masked gunman robs third bank.** A masked gunman robbed the TCF Bank in St. Anthony, Minnesota March 1 and is suspected of a similar robbery February 28, and another January 3, the FBI said. The suspect robbed the TCF Bank on Silver Lake Road about 7 p.m. He displayed a handgun in the lobby, ordered everyone to lie on the floor and demanded money from a teller, according to an FBI news release. He fled on foot. The man is also suspected of robbing the TCF Bank on Suburban Avenue in St. Paul February 28. He also brandished a gun in that incident. He is also a suspect in the TCF Bank robbery in West St. Paul January 3. The suspect is described as an Asian man, 5 foot 7, wearing all black clothes and a black mask. Source: http://www.startribune.com/local/stpaul/117266618.html

National

E. coli found on 50 percent of shopping carts. Researchers from the University of Arizona swabbed shopping cart handles in four states looking for bacterial contamination. Of the 85 carts examined, 72 percent turned out to have a marker for fecal bacteria. The researchers took a closer look at the samples from 36 carts and discovered Escherichia coli, more commonly known as E. coli, on 50 percent of them — along with a host of other types of bacteria. "That's more than you find in a supermarket's restroom," said the lead researcher on the study and a professor of microbiology at the University of Arizona. The study's results may explain earlier research that found that kids who rode in shopping carts were more likely than others to develop infections caused by bacteria such as salmonella and campylobacter, the lead researcher said. Source: http://www.msnbc.msn.com/id/41838546/ns/health-kids_and_parenting/

FBI crime report highlights trends in Internet fraud. The recently published FBI 2010 Internet Crime Report reveals the most common types of Internet crimes in 2010 were non-delivery of payment or merchandise, impersonating the FBI, and identity theft. According to the joint FBI/National White Collar Crime Center's Internet Crime Complaint Center (IC3), it received more than 300,000 complaints about these particular Internet scams and more. The majority of the filings came from U.S. males between the ages of 40 and 59 years old with targets primarily in California, Florida, Texas, and New York. International complaints came from Canada, the United Kingdom, Australia, and India. In the cases actually solved by the FBI or local law enforcement officials, the majority of perpetrators (around 75 percent) were males residing in California, Florida, New York, Texas, the District of Columbia, and Washington state. Internationally, the hotbeds for scammers were in the United Kingdom, Nigeria, and Canada. The top ten crimes were: computer crimes, miscellaneous fraud, advance feed fraud, spam, auction fraud, credit card fraud, and overpayment fraud. These crimes

were mostly carried out through telephone calls claiming victims are delinquent on payday loans and should pay right away, online apartment and real estate scams, denial of service attacks on cell phones and landlines targeting bank accounts, as well as fake emails asking for donations for natural disasters like Hurricane Katrina and the tsunamis. Source: http://www.tgdaily.com/security-features/54342-fbi-crime-report-highlights-trends-in-internet-fraud

INTERNATIONAL

Gaddafi strikes oil areas, Arabs weigh peace plan. The Libyan leader's forces struck at rebel control of oil export hubs in Libya's east for a second day on March 3 as Arab states weighed a plan to end turmoil Washington D.C. officials said could make the nation "a giant Somalia." A leader of the uprising against the Libyan leader's 41-year-old rule said he would reject any proposal for talks with him to end the conflict in the world's 12th largest oil exporting nation. Witnesses said a warplane bombed the eastern oil terminal town of Brega, a day after troops loyal to Libya's leader launched a ground and air attack on the town that was repulsed by rebels spearheading a popular revolt against his four-decade-old rule. Rebels called on March 3 for a no-fly zone, echoing a demand by Libya's deputy U.N. envoy, who now opposes the Libyan leader. A rebel officer said government air strikes targeted the airport of Brega and a rebel position in the nearby town of Ajdabiyah, referring to two rebel-held locations. Opposition soldiers also said troops loyal to the Libyan leader had been pushed back to Ras Lanuf, home to another major oil terminal and 600 kilometers east of Tripoli. Source: http://www.publicbroadcasting.net/wfsu/news.newsmain/article/0/0/1770307/World/Gaddafi.strikes.oil.areas..Arabs.weigh.peace.plan

Two U.S. troops killed in Germany airport shooting, police say. A 21-year-old man from Kosovo is in custody after two American troops were killed and two others were wounded March 2 in a shooting incident on a U.S. military bus at Germany's Frankfurt Airport, authorities said. Police said they believe the suspect stormed onto the bus, which was waiting at the terminal, and began shooting. The suspect is from the northern town of Mitrovica, Kosovo's interior minister said, citing the U.S. Embassy in Pristina as his source. The suspect has passports from Germany and from Yugoslavia, the latter of which was issued prior to Kosovo's declaration of independence from Serbia in 2008, the interior minister said. Officials were running a background check on the suspect, who lives in Germany, for possible terrorist links. CNN was not able to reach anyone at the U.S. Embassy for comment. A U.S. military official said the bus driver was among the dead. Both fatalities were U.S. Air Force airmen from Lakenheath base in Britain. The two wounded were security forces who were on their way to a deployment, said the source. FBI agents were on the scene shortly after the shooting occurred. Source:
http://www.cnn.com/2011/WORLD/europe/03/02/germany.shooting/index.html?hpt=T1

14 killed in Mexico bar attacks. At least 14 people were killed in three separate attacks in bars in northern Mexico, authorities said February 27. In Coahuila state, across the border from Texas, nine men died February 26 when gunmen opened fire inside two bars in separate attacks, state prosecutors said in a statement. Eleven others were wounded. Assailants killed another five men February 26 in a bar in Ciudad Juarez, a Chihuahua state prosecutors' spokesman said. Source: http://www.wral.com/news/national_world/world/story/9183976/

Banking and Finance Industry

Cybercriminals targeting point-of-sale devices. Point-of-sale (POS) payment processing devices for credit and debit cards are proving to be rich targets for cybercriminals due to lax security controls, particularly among small businesses, according to a report from Trustwave. Trustwave, which investigates payment card breaches for companies such as American Express, Visa, and MasterCard, conducted 220 investigations worldwide involving data breaches in 2010. The vast majority of those cases came down to weaknesses in POS devices. "Representing many targets and due to well-known vulnerabilities, POS systems continue to be the easiest method for criminals to obtain the data necessary to commit payment card fraud," according to Trustwave's Global Security Report 2011. POS devices read the magnetic stripe on the back of a card that contains account information, which is then transmitted for payment processing. Although there are rules for security controls developers should use for the devices, such as the Payment Application Data Security standard (PA-DSS), Trustwave said "these controls are rarely implemented properly." POS devices are an attractive target for cybercriminals since the data they access from the cards is more complete, Trustwave said. Source: http://www.computerworld.com/s/article/9212882/Cybercriminals_targeting_point_of_sale_devices

Morgan Stanley attacked by China-based hackers who hit Google. Morgan Stanley experienced a "very sensitive" break-in to its network by the same China-based hackers who attacked Google Inc.'s computers more than 1 year ago, according to e-mails stolen from a cyber-security company working for the bank. The e-mails from the Sacramento, California-based computer security firm HBGary Inc., which identify the first financial institution targeted in the series of attacks, said the bank considered details of the intrusion a closely guarded secret. "They were hit hard by the real Aurora attacks (not the crap in the news)," wrote a senior security engineer at HBGary, who said he read an internal Morgan Stanley report detailing the so-called Operation Aurora attacks. The nickname came from McAfee Inc., a cyber-security firm, which said the attacks occurred for about 6 months starting in June 2009 and marked "a watershed moment in cyber security." The number of companies known to be hit in the attacks was initially estimated at 20 to 30 and now exceeds 200, said the senior vice president for Terremark Worldwide Inc., which provides information-technology security services. The HBGary e-mails do not indicate what information may have been stolen from Morgan Stanley's databanks or which of the world's largest merger adviser's multinational operations were targeted. Source: http://www.bloomberg.com/news/2011-02-28/morgan-stanley-network-hacked-in-same-china-based-attacks-that-hit-google.html

FFIEC draft puts more responsibility on banks. A preliminary draft of new online authentication guidance from the Federal Financial Institutions Examination Council (FFIEC) puts greater responsibility on financial institutions to enhance their security and prevent fraud. The FFIEC has yet to formally unveil its long-awaited update to 2005's authentication guidance, but a December 2010 draft document entitled "Interagency Supplement to Authentication in an Internet Banking Environment" was distributed to FFIEC's member agencies — the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corp., Office of the Comptroller of the Currency, National Credit Union Administration, and Office of Thrift Supervision — for review and comment. Copies of this draft circulated within the banking and security communities recently, and two were sent separately and anonymously to Information Security Media Group. While it is likely this draft will be amended before the final release of the new guidance, the current document calls for five key areas

of improvement: (1) Better risk assessments to help institutions understand and respond to emerging threats, including man-in-the-middle or man-in-the-browser attacks, as well as keyloggers; (2) Widespread use of multifactor authentication, especially for "high-risk" transactions; (3) Layered security controls to detect and effectively respond to suspicious or anomalous activity; (4) More effective authentication techniques, including improved device identification and protection, as well as stronger challenge questions; (5) Heightened customer education initiatives, particularly for commercial accounts. Source: http://www.bankinfosecurity.com/articles.php?art_id=3374

Fake ACH transfer failure notifications spread ZeuS. A new wave of spam e-mails are targeting business users and attempt to infect them with a variant of the ZeuS banking trojan by posing as ACH transfer failure notifications. According to researchers from antivirus vendor Trend Micro who analyzed the campaign, the e-mails purport to come from NACHA — The Electronic Payments Association, the regulatory agency for the Automated Clearing House (ACH) network. The ACH network is commonly used by companies to process large volumes of credit and debit transactions, such as payroll or vendor payments, in batches. According to the director of research in computer forensics at the University of Alabama at Birmingham, the e-mails have subjects such as "ACH transaction cancelled", "ACH Transfer rejected", "Your ACH transaction," and other such variations. Source: http://news.softpedia.com/news/ACH-Transaction-Failure-Notifications-Spread-ZeuS-186368.shtml

New banking trojan targets all major browsers. Spanish security firm S21sec has identified a new banking trojan capable of injecting HTML into all popular browsers which uses a rootkit to hide its components. Dubbed Tatanga, the trojan is written in C++ and is organized in modules with different functionality which are decrypted in memory as needed. Like other banking trojans, Tatanga executes Man-in-the-Browser (MitB) attacks in order to perform unauthorized transactions from the accounts of its victims. The trojan currently targets banks from Western European countries, particularly the United Kingdom, Germany, Spain, and Portugal. It currently has a very low detection rate. A signature-based Virus Total scan revealed that only 9 in 43 antivirus engines currently detect the infector as malicious and most of them do it under generic names. Microsoft calls it Trojan:Win32/Mariofev(dot)B and first added detection for it in September. However, the definition was updated the week of February 21, probably to account for new variants. According to S21sec researchers, the trojan comes with an e-mail harvesting module, one that handles encrypted communication, another for the removal of competing trojans, including ZeuS, a module for blocking antivirus programs, one handling the encrypted configuration file, the HTML injector, and a file patcher. Source: http://news.softpedia.com/news/New-Banking-Trojan-Targets-All-Major-Browsers-186443.shtml

Chemical and Hazardous Materials Sector

Scientists want to help regulators decide safety of chemicals. Groups representing 40,000 researchers and clinicians are urging federal agencies responsible for the safety of chemicals to examine the subtle impact a chemical might have on the human body rather than simply ask whether it is toxic. In an open letter to the Food and Drug Administration and the Environmental Protection Agency to be published March 4 in the journal Science, the scientists said regulatory agencies must tap into genetics, developmental biology, endocrinology, and other disciplines when they analyze the safety of chemicals used in everyday products. "Although chemical testing and risk assessment have

long been the domain of toxicologists, it is clear the development of improved testing guidelines and better methods of assessing risks posed by common chemicals to which all Americans are exposed requires the expertise of a broad range of scientific and clinical disciplines," said the letter, which was signed by eight scientific societies. Source: http://www.washingtonpost.com/wp-dyn/content/article/2011/03/03/AR2011030306639.html

BPA-free plastic may release chemicals with estrogenic activity. The estrogenic chemical bisphenol-A (BPA) has been villified in recent years for its ubiquitous presence in numerous consumer products. But even plastic-containing products claiming to be BPA-free can leach chemicals with estrogenic activity (EA), according to a new study published in the Environmental Health Perspectives Journal. The leaching can get worse during regular types of use, such as microwaving or dishwashing. Researchers at Georgetown University, PlastiPure, a Texas-based plastic maker, and CertiChem, a chemical testing firm, purchased 455 plastic products made to contain food, including baby bottles, water bottles, bags and deli containers. The resin type varied, but nearly all tested positive for the leaching of chemicals with detectable levels of EA. Studies suggest exposure to EA can change the structure of many types of human cells, raising concern about adverse impacts on infants and children, including birth defects and behavioral disorders. However, researchers contend EA-free plastic can be commercially produced at a cost in line with conventional plastic. "Many scientists believe that it is not appropriate to bet our health and that of future generations on an assumption that known cellular effects of chemicals having EA released from most plastics will have no severe adverse health effects," researchers wrote. "Since we can identify existing, relatively-inexpensive monomers and additives that do not exhibit estrogenic activity, even when stressed, we believe that plastics having comparable physical properties but that do not release chemicals having detectable EA could be produced at minimal additional cost." Source: https://www.greenbiz.com/news/2011/03/03/bpa-free-plastics-release-chemicals-estrogenic-activity

(Illinois) **Illinois' oversight of nuclear power plants falls through the cracks.** Four of Illinois' nuclear power plants, including the facility in Byron, were not properly inspected by the Illinois Environmental Protection Agency (IEPA). That is according to a report by the state auditor general. The IEPA said many of their workers simply did not know how to do the inspections. "We didn't have staff trained in how to do this, we now do have fully trained staff and have added another staff person and all the inspections are being done, per the new law," an IEPA spokesman said. In 2008, a new law required the IEPA to do quarterly safety inspections. Their role, to check records and see if wells containing radioactive material are leaking any of the toxic liquid. A danger the IEPA spokesman said never panned out. "I'm not aware of any danger or even any contamination of wells," the IEPA spokesman said. While the state failed to do their inspections, the crew that operates the Byron facility did not. A Byron power plant spokesperson released this statement: "Byron Station had zero reportable environmental events in 2010 and our records are always available at any time for state inspections." Source: http://mystateline.com/fulltext-news?nxd_id=233006

Commercial Facilities

Building codes increasingly unable to withstand extreme weather. Basic infrastructure around the world has had increasing difficulty in withstanding more extreme weather patterns. With record snow falls in the Northeastern United States, hundreds of roofs have collapsed under the weight of

snow showering bystanders with debris and even crushing cows and tractors. In a high profile case, the Metrodome collapsed after 18 inches of heavy snow fell in Minneapolis, while in Hungary, several weeks of sustained rainfall caused a wall holding toxic red sludge to collapse, sending a torrent of toxic waste into nearby villages. The increasing prevalence of these types of infrastructure failures has engineers and insurers worried. Many believe global warming is behind the increasing frequency of extreme weather events such as floods, storms, and droughts that have strained infrastructure. According to Munich Re, one of the world's largest insurance companies, weather-related incidents serious enough to cause property damage have risen sharply since 1980. The company said that extreme floods and windstorms have approximately tripled, while the number of days with heavy rainfall in South America, North America, and parts of Europe has also increased. Source: http://homelandsecuritynewswire.com/building-codes-increasingly-unable-withstand-extreme-weather

Communications Sector

FCC votes to review TV retransmissionnegotiation rules. The Federal Communications Commission (FCC) made no immediate changes to retransmission rules March 3, but the panel's members warned broadcasters and cable companies not to use the FCC's decision to review the rules as an excuse to back out of negotiations. The commission unanimously voted to consider and seek comment on potential changes to TV retransmission rules, which govern how cable companies or other video distributors retransmit broadcast stations. Recent high-profile disputes between cable and satellite TV carriers and broadcasters have led to millions of viewers in the dark when programming is pulled. And right now a spat between Dish Network Corp. and Lin TV Corp. is threatening to cause another "blackout." Among the potential changes to be examined are measures that would provide more guidance about good-faith negotiating requirements, improve notice requirements for consumers, and eliminating rules that provide for contract enforcement through the FCC, rather than through the courts. Source: http://techdailydose.nationaljournal.com/2011/03/fcc-votes-to-review-tv-retrans.php

FCC to study rules on cable-broadcast negotiations. The Federal Communications Commission is set to vote March 3 to launch a review of the federal rules that govern negotiations over the fees that cable, satellite, and other video services pay TV stations to carry their signals in channel lineups. To supplement advertising revenue, broadcasters have begun demanding cash for signals they used to give away for free, and that contributes to rising cable bills. The FCC's actions follow a series of high-profile standoffs that left some consumers without their local stations. In October, a breakdown in negotiations between Cablevision Systems Corp. and News Corp.'s Fox network left 3 million Cablevision subscribers in the New York area without Fox programming for 15 days — including through two World Series games — after the broadcaster pulled its signal. The FCC wants to examine its existing rules to determine if there are other ways to prevent impasses by ensuring that both sides negotiate in good faith. Source: http://www.boston.com/business/technology/articles/2011/03/02/fcc_to_study_rules_on_cable_broadcast_negotiations/

Critical Manufacturing

Spiders lead to Mazda recall. Mazda is recalling about 52,000 Mazda6 sedans, because spiders like to build their nests in part of the fuel system. "A certain type of spider may weave a web in the evaporative canister vent line and this may cause a restriction of the line," Mazda said in a letter to the National Highway Traffic Safety Administration. The evaporative canister vent line runs from a charcoal-filled canister that cleans air coming out of the gas tank. Blockage of the line can prevent air from getting into the gas tank as the gasoline is used, resulting in negative air pressure inside the tank. That can lead to a crack in the gas tank and the possibility of a fire. No actual fires are known to have been caused by the spiders, according to Mazda's letter. Dealers will inspect and, if necessary, repair the fuel system in the cars. A spring will also be installed to prevent spider intrusion, according to the letter. Letters will be mailed to owners of affected vehicles beginning at the end of March. Source: http://money.cnn.com/2011/03/03/autos/mazda6_spider_recall/index.htm?hpt=T2

Ford recalls vehicles over fuel leaks. Ford Motor Co. is recalling about 35,000 pickup trucks and crossover vehicles in the United States and Canada because of possible fuel leaks and electrical shorts that could lead to fires. Ford says the recall includes about 25,000 2010 Ranger pickups and involves fixing potential problems with the fuel line that could lead to a fuel leak and a fire. No fires or injuries have been reported. Ford also is recalling more than 9,000 other vehicles to fix a software problem that could lead to an electrical short and overheating, potentially causing a fire. The recall involves 2011 model years of the Ford Edge, F150, F250, F350, F450, F550, and Lincoln MKX. Ford says it does not know of any incidents related to the recalled vehicles. Source: http://www.google.com/hostednews/ap/article/ALeqM5iS1dQfzthcVxcGrN2WEJR-ln_hKw?docId=be2af46c5cbf4984a4723f2645e6838a

Burlington Coat Factory recalls slow cookers due to fire hazard. Burlington Coat Factory, of Burlington, New Jersey, has issued a recall March 2 for about 7,460 slow cookers. The importer/distributor was Lehrhoff ABL, of Carlstadt, New Jersey. The slow cooker's control panel can overheat and melt, posing a fire hazard. The manufacturer has received 60 reports of the control panels smoking, melting and sparking, and three reports of panels catching fire. Fourteen incidents resulted in minor damage to countertops. No injuries have been reported. This recall involves Bella Kitchen 5-quart programmable slow cookers. The slow cookers were sold at Burlington Coat Factory stores from June 2010 through December 2010. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml11/11150.html

Defense/ Industry Base Sector

NASA satellite launch goes awry. A rocket carrying an Earth-observation satellite likely is in the Pacific Ocean after a failed launch attempt, NASA officials said March 4. The Taurus XL rocket carrying the National Aeronautics and Space Administration's Glory satellite lifted off around 2:10 a.m. Pacific time from Vandenberg Air Force Base in California. Officials explained at a news conference that a protective shell or fairing atop the rocket did not separate from the satellite as it should have about 3 minutes after the launch. That left the Glory spacecraft without the velocity to reach orbit. Source: http://online.wsj.com/article/SB10001424052748703580004576180252332597670.html

Company plans fixes for JSF helmet display issues. Fixes are in the works for several technical glitches that have been plaguing the helmet-mounted display in F-35 fighter jets, said an official from Vision Systems International, which builds the unit. Among the problems pilots have complained of are latency — where the imagery does not keep up with the motion of the pilots head, imagery that is misaligned with the pilot's vision, and jittery images. The problem is especially pronounced with the helmet's night-vision system, which is meant to display images from six infrared cameras mounted around the aircraft's fuselage, the Joint Strike Fighter program chief said. The program has been looking at alternative night-vision systems for the first training unit, scheduled to receive its first F-35s in May. The program chief said near-term fixes could include moving the imagery to the aircraft's head-down flat-panel displays, and having pilots use conventional night-vision goggles. But these are not satisfactory long-term solutions, he said. The president of Vision Systems International said the company has long-term solutions mapped out. Source: http://www.defensenews.com/story.php?i=5828022&c=AME&s=AIR

Broomall man convicted of shipping equipment to Iran. An Iranian national who has lived in the United States for more than 20 years was convicted February 24 of exporting banned material to his homeland, including sophisticated laboratory equipment, laptop computers, and fuel cells. The verdict against the man, 43, followed 6 days of deliberations over 2 weeks, and a lengthy trial that started in January. The man and a partner, 44, who pleaded guilty in 2010, operated Saamen Co. L.L.C. in Newtown Square, Pennsylvania, which exported the equipment to Dubai, where coconspirators shipped it on to Iran. In 2003, The man's Iranian contacts asked the 2 men to try to obtain 134 American helicopter pilot helmets. The case involved investigators from the FBI, Immigration and Customs Enforcement, and the Department of Commerce. The men also shipped items such as ultrasonic liquid processors and hydrophones, according to prosecutors. Source: http://articles.philly.com/2011-02-25/news/28629792_1_illegal-exports-broomall-man-iran

Emergency Services

(New York) **N.Y. police: Gunman had planned mass murder.** A heavily armed man who crashed his pickup truck in Bellmore, New York, then shot an emergency medical technician (EMT) responding to the accident before being killed by police, appeared to be planning a mass killing, police said March 2. The man had a rifle strapped to his chest, and extra ammunition inserted in elongated wristbands on his arms, the Nassau County Police Commissioner told reporters. He had six weapons in his possession, including a Tec-9 automatic pistol. Shooting erupted at about 10 p.m. March 1, after the man hit a utility pole with his truck. When the volunteer ambulance crew arrived, he fired at least eight shots at them from an assault rifle, wounding the EMT. Police responding to the crash then fatally shot the man when he threatened them. Source: http://officer.com/online/article.jsp?siteSection=1&id=57108

(New York) **Mohamed Diallo, Kwamell Smith try to pass as FBI agents, city police say.** Two men were charged March 2 after they allegedly attempted to impersonate FBI agents while possessing stolen weapons in Rochester, New York. The men were charged with three counts of second-degree criminal possession of a weapon, and two counts of fourth-degree criminal possession of stolen property. An officer was on patrol near East Main Street and Culver Road March 1 when he observed a sport utility vehicle being operated with a blue LED dash light. Two officers followed the SUV and tried to stop it.

A brief chase ended when the driver lost control of the vehicle. The passenger ran away but was apprehended after a brief chase. Police recovered an "FBI" jacket and three handguns, two of which were reported stolen. The jacket was not authentic. Police are investigating whether the two men could have been involved in connection with a similar incident on Cedarwood Avenue. During the arrest, a Rochester resident called 911 to say he had been followed by an SUV on Cedarwood Avenue, where two men dressed as FBI agents approached him and ordered him to stop. The Rochester resident ran into a home and the men drove away. The FBI has been notified and may pursue further charges at a later date, an official said. Source: http://www.democratandchronicle.com/article/20110303/NEWS01/103030334/1003/news01/Mohamed-Diallo-Kwamell-Smith-try-pass-FBI-agents-city-police-say

(Texas) **National guardsmen among McAllen drug, guns bust.** A National Guardsman is among several people arrested in a drug bust in McAllen, Texas, where authorities also found guns and bulletproof vests headed to Mexico. Investigators told media sources that the guardsman allegedly supplied those items and other military articles to the suspects in a gun and drugs ring. Police said they raided two different locations in McAllen, where they arrested a total of 11 people. During their search, police seized assault rifles, guns, ammunition, and grenades. All were headed to Mexico. Police also recovered several tons of marijuana and over 1,000 pounds of cocaine. The McAllen police chief said the investigation is still not complete and more arrests could be made. Source: http://www.valleycentral.com/news/story.aspx?list=195030&id=585549

(Wisconsin) **Milwaukee police system pinpoints gunfire.** A high-tech, federally funded system of sensors and software now allows Milwaukee, Wisconsin police to pinpoint exactly where in one violent area of the city shots have been fired — and to get officers there in a hurry. The system, supplied by a Mountain View, California company, detects the shock waves from a bullet being fired and can sort that information out from all the other noise in the area, company officials said. It then transmits the data to dispatchers in the police department's communications center, who see the location of the shooting on a screen, hear the shots, and can immediately send officers to the scene. The sensors are attached to buildings in the area, with permission of the owners. The system has picked up 101 shots over the past 30 days in the neighborhood, according to police — and generated 200 dispatch calls to officers since it was first tried December 24. Source: http://officer.com/online/article.jsp?siteSection=1&id=57035

ENERGY

(New York) **21,000 worth of copper wire reported stolen at EPCAL one day after substation vault fire.** The theft of $21,000 worth of copper wire at the Calverton Enterprise Park (EPCAL) in Riverhead, New York, was reported to Riverhead Town Police February 25, 1 day after an underground fire at the Long Island Power Authority substation at the site cut power to the entire industrial park. The theft occurred between December 1, 2010 and February 25, when a site manager discovered it, the police report said. Thieves made off with about 1,000 feet of copper wire, taken from within an above-ground outside conduit that ran from a service panel off Scott Avenue to an office trailer, police said. The lock to the trailer was also cut, and a $100 tool box was stolen. Police said the perpetrator(s) accessed the property, which is surrounded by a chain-link fence, by cutting a hole in the fence. There was no alarm or surveillance system on the property, according to the police report. The site is one of

several at EPCAL still owned by the U.S. Navy, which retained certain parcels on the former Grumman site for environmental remediation subsequent to transferring 2,900 acres to the Town of Riverhead in 1998. Source: http://www.riverheadlocal.com/local-news-content/1715-major-copper-wire-theft-at-epcal

Food and Agriculture

(New Jersey) **Customs officials discover destructive beetle larva.** U.S. Customs and Border Protection agriculture specialists discovered Khapra Beetle larva while inspecting a ship's cargo at the port in Elizabeth, New Jersey, officials announced March 2. The Khapra Beetle is one of the world's most destructive pests of grain products and seeds. During a February 15 inspection of the vessel's dry provisions stores, a small unlabeled plastic bag of dried black beans showed signs of infestation. An adult insect, casts, and several live larvae were found inside the bag, officials said. A sample was collected and sent to U.S. Department of Agriculture (USDA) entomologists for final determination. USDA identified the sample as Trogoderma granarium. Treatment according to USDA standards must be performed on the vessel before it can return to a U.S. port. A Customs official will board the vessel upon arrival, and proof of treatment must be made available. Source: http://njtoday.net/2011/03/03/customs-officials-discover-destructive-beetle-larva/

(Florida) **Avocado pest found near south Florida production area.** Agriculture inspectors have spotted the presence of a tree-killing disease close to south Florida's avocado production region. The Florida Department of Agriculture and Consumer Services has discovered laurel wilt disease, a fungus that destroys red bay and avocado trees, on three swamp bay trees in south Miami-Dade County. The finding is 7 miles north of the state's commercial avocado production region near Homestead and Florida City. An administrator of the Florida Avocado Administrative Committee, Homestead, said the finding was not too far south of where trappers in 2010 spotted the bug in the central-west side of Miami-Dade County. "No one is panicking," the administrator said. "It's not near the growing area yet and (the finding) is just an informational thing." The public information director with the Tallahassee-based agency said inspectors will begin aerial surveys to determine how far the disease has spread. She said the department met with an industry working group February 25 to address concerns on what the agency is doing to increase trapping and prevent the advance of the disease, which is spread by the redbay ambrosia beetle. Source: http://thepacker.com/Avocado-pest-found-near-south-Florida-production-area/Article.aspx?oid=1310342&fid=PACKER-CROPS-AND-MARKETS&aid=657

(Ohio) **Ohio Fresh shipped contaminated eggs.** Ohio Fresh Eggs, of Johnstown, Ohio, knew its product had tested positive for Salmonella Enteritidis (SE), but 798 cases of eggs that should have been treated for the bacteria were instead shipped to the nation's largest distributor of shell eggs, Cal-Maine Foods. The egg producer February 25 received a warning letter from the U.S. Food and Drug Administration (FDA). Ohio Fresh, in a response published in the Des Moines Register said eggs from one barn had been shipped accidentally. FDA investigators, who arrived at Ohio Fresh November 2 discovered the contaminated eggs had been shipped and alerted Cal-Maine, a company that produces, grades, packs, and sells table eggs in 29 states. By that time Cal-Maine, which received the contaminated eggs for processing and re-packaging between October 9 and 12, 2010, had already distributed the bad eggs to Arkansas, California, Illinois, Iowa, Kansas, Missouri, Oklahoma, and Texas.

It was forced to recall 24,000 dozen eggs November 5, 2010. Source: http://www.foodsafetynews.com/2011/03/ohio-fresh-shipped-eggs-it-knew-where-contaminated/

GAO report calls for single food safety agency. In a sweeping report on how to carve as much as $200 billion out of the federal government, the General Accountability Office (GAO) said there should be just one federal food safety agency, even if consolidating the now fragmented system does not save much, if any, money. GAO, in its first annual report to Congress to identify federal programs, agencies, offices, and initiatives that have duplicative goals or activities, led off with the inefficiency of supporting 15 federal food safety agencies. The sponsor of the legislation that called for the new report, released March 1, was an Oklahoma Senator, a critic of the recently enacted Food and Drug Administration (FDA) Food Safety Modernization Act who emerged as the Senate's biggest deficit hawk. "Fragmented food safety system has caused inconsistent oversight, ineffective coordination, and inefficient uses of resources," GAO reported. "The Department of Agriculture's (USDA) Food Safety and Inspection Service and the Food and Drug Administration are the primary food safety agencies, but 15 agencies are involved in some way." GAO said it takes 15 federal agencies to collectively administer at least 30 food-related laws, with budget obligations for USDA's Food Safety and Inspection Service (FSIS) and FDA totaling over $1.6 billion in fiscal year 2009. Source: http://www.foodsafetynews.com/2011/03/call-for-one-food-safety-agency-leads-historic-gao-report/

USDA inspector general questions E. coli testing. The U.S. Department of Agriculture's Inspector General (IG) questioned the validity of the Food Safety and Inspection Service (FSIS) E. coli O157:H7 sampling program, raising questions about meat safety at a time when Congress is considering cutting the FSIS inspection budget. In testimony March 2 before the House Agriculture Appropriations subcommittee, the IG told lawmakers her office completed an audit to assess FSIS' sampling program for beef trim — currently inspectors take 60 samples from large lots of beef trim to test for E. coli O157:H7 — and determined the current method "does not yield a statistical precision that is reasonable for food safety." The IG noted FSIS "generally agreed" with her office's findings and recommendations. She said her office had also begun a review of FSIS E. coli testing protocols to ensure beef trim is "effectively collected and analyzed." Source: http://www.foodsafetynews.com/2011/03/usda-inspector-general-questions-e-coli-testing-program/

(California) **Calif food supplier recalls chicken, pork products.** Taylor Farms Pacific of Tracy, California, recalled 64,000 pounds of chicken and pork products because some broccoli in the products was found to be contaminated with listeria. The United States Department of Agriculture (USDA) said March 1 that several premade dishes were found to have contamination after routine testing. The USDA says each item bears the establishment number "P-34013" or "EST. 34013" inside the department's mark of inspection. The products were produced between February 6 and February 23 and shipped to Arizona, California, Colorado, and Wyoming. The agency says it has not received reports of anyone sickened as a result of the contamination. Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2011/03/01/state/n220057S32.DTL

California firm recalls chicken and mushroom pie products due to mislabeling and undeclared allergen. Piccadilly Fine Foods, a Santa Clara, California establishment, recalled about 775 pounds of chicken and mushroom pie products because they may contain an undeclared allergen, egg, the U.S.

Department of Agriculture's Food Safety and Inspection Service (FSIS) announced February 28. The following products are subject to recall: 12-pound cases of "Piccadilly Fine Foods Chicken and Mushroom Pastie" with each case containing 24 individual packages. The chicken-and-mushroom pies were produced on various dates between August 1, 2010 and February 25, 2011. But some products subject to recall during this time frame are correctly labeled in that they do include "egg" in the ingredient statement. The products were shipped to distributors in California, Colorado, Florida, and Texas for further distribution to retail outlets.Source: http://www.fsis.usda.gov/News_&_Events/Recall_015_2011_Release/index.asp

(Virginia; New York) **New Market Poultry recalls chicken.** New Market Poultry, a New Market, Virginia establishment, is recalling about 3,339 pounds of ice-packed, whole chicken products that may be adulterated due to leaking cooler condensate, the U.S. Department of Agriculture's (USDA) Food Safety and Inspection Service (FSIS) announced February 25. The problem was identified February 24 when the company discovered products under the USDA retention had been shipped. FSIS personnel observed February 23 standing water with unidentified black specks pooling on the box lids of the packed chickens stored in a company cooler. The palletized boxes, which contain drainage holes, were retained by FSIS and should not have been shipped. Each box bears the establishment number "P-4602A" inside the USDA mark of inspection. The chicken products were produced on February 23 and inadvertently shipped the same day to six distribution centers in the Bronx, Brooklyn, and Farmington, New York. Source: http://www.foodpoisonjournal.com/food-recall/new-market-poultry-recalls-chicken/

Appeals court overturns sugar beet injunction. Environmental groups failed to show that seed plants for sugar beets genetically modified to withstand the popular weed killer Roundup would cause irreparable harm, a federal appeals court said February 25 in overturning an injunction that called for the destruction of the plants. The 9th U.S. Circuit Court of Appeals in San Francisco, California said it disagreed with a federal district court decision last fall granting the injunction against the planting of the seed plants, also called stecklings. "We conclude the district court abused its discretion in granting a preliminary injunction requiring destruction of the steckling plants," the court wrote. "Plaintiffs have not demonstrated that the ... plants present a possibility, much less a likelihood, of genetic contamination or other irreparable harm. The undisputed evidence indicates that the stecklings pose a negligible risk of genetic contamination, as the juvenile plants are biologically incapable of flowering or cross-pollinating before February 28, 2011, when the permits expire." The decision was the latest in the ongoing dispute over the genetically altered sugar beets, which were developed by Monsanto. Source: http://www.ajc.com/news/nation-world/appeals-court-overturns-sugar-853733.html

St. Paul distributor recalls cheese dip. A St. Paul, Minnesota distributor recalled about 87 pounds of buffalo chicken cheese dip because the label does not list MSG that is contained in the product. J&J Distributing is recalling 16-ounce metal containers of "Cub Fresh Buffalo Chicken Cheese Dip" and 16-ounce metal containers of "Kowalski's Markets Buffalo Chicken Cheese Dip." The dip was shipped to retailers in the Minneapolis, Minnesota area and has sell-by dates ranging from February 23 to February 25. Source: http://www.postbulletin.com/news/stories/display.php?id=1446346

Government Sector (including Schools and Universities)

U.S. Navy officer charged with espionage. A U.S. Navy intelligence specialist was charged March 3 with espionage after he allegedly tried to sell classified information to an undercover FBI agent, officials said. The Specialist 2nd Class faced charges of attempting to forward classified information to a person not authorized to receive such information, the U.S. Navy said in a statement. A court-martial date has not yet been set, but the man was charged with 4 specifications of attempted espionage, and 11 specifications of mishandling classified information. FBI and Naval Criminal Investigative Service agents apprehended the man December 1 in Fayetteville, North Carolina, after being suspected of trying to sell information marked "secret" and "top secret." He is currently held at Naval Brig Norfolk in Virginia. All charges stemmed from incidents that took place when the man was assigned to the Expeditionary Combat Readiness Center at Joint Expeditionary Base Little Creek in Fort Story, Virginia, according to the Navy. Source: http://www.google.com/hostednews/afp/article/ALeqM5iInttW6TvVzQ2pZV5SAPFcNTHosg?docId=CNG.392b3b6876d28b9fdef7cc1c3a51c09d.2b1

(Texas) **Student poisoned teacher, investigators say.** A teacher from Plumb Creek Elementary in Joshua, Texas is recovering after drinking some tainted tea. Law enforcement officials said she was poisoned by one of her students. The sixth grade teacher became violently ill the night of March 1. The same day, investigators from the Johnson County Sheriff's Department said one of her students spiked her drink with a chemical used in detergents. "The student was able to obtain sodium carbonate from a science kit in a small quantity and put it into tea the teacher was drinking," a police captain said. In a small dose, the chemical can make a person sick; in large doses it can by deadly. When the teacher did not show up at school March 2, some of her students became concerned because they had heard about the poisoning plot, so they told administrators. The police captain said initially the 12-year-old boy responsible denied it. But eventually he admitted putting the sodium carbonate in the drink. The boy is being held in a juvenile detention facility. He is charged with assault on a public servant. Source: http://www.myfoxdfw.com/dpp/news/education/030311-student-poisoned-teacher,-investigators-say

(Texas) **ATF: Gun in US agent's death traced to Texas man.** Three people suspected of smuggling guns to Mexico were arrested in a Dallas, Texas suburb February 28 after federal investigators traced the gun used in the killing of a U.S. agent in Mexico to one of them, officials said. Agents of the U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) arrested the suspected gun smugglers in morning raids in the southern Dallas suburb of Lancaster, an ATF spokesman said. The ATF said the gun was used in the February 15 shooting of two federal agents who were driving on a highway near the northern city of San Luis Potosi, where one agent was killed and the other was wounded. Also, the Mexican navy announced February 28 marines had captured a regional boss for the drug gang that is accused in the agent's slaying. The regional boss and five other suspects, including a Honduran man, were detained February 27 at a hotel in Saltillo, capital of the northern state of Coahuila. Federal agents said the suspect also is suspected in the February killing of a retired army general who recently had become police chief in Nuevo Laredo, the city across the border from Laredo, Texas. Source:

http://www.google.com/hostednews/ap/article/ALeqM5glPqz_K6pqQSlL4d9sUQFFxONfDQ?docId=6cd4903cd80749b88385c3699355a4bb

(California) **CCTV cameras on campus are catching crime.** Closed circuit television (CCTV) cameras are recording activity on a 24-hour basis on every campus at Santa Monica College (SMC) in Santa Monica, California. The cameras have assisted with catching criminal activity in cases dating as recently as February 23. The first cameras were set up 20 years ago following an incident involving a student entering the bookstore with a handgun. The camera collection has accumulated over the years and now totals up to 300 cameras district-wide, according to a SMC police officer. The officer described the surveillance system's purpose to have three main components: deterring future crime, monitoring for crime, and case investigation. If and when a crime is captured on film, the police respond promptly by raising awareness of the incident through bulletins and notices, as explained by a facilities manager. Depending on circumstances, police may respond with an increase in patrol and the footage archived for investigation. Although the cost of the entire CCTV system was not determined, the dispatch center's recent renovation from analog to digital system was roughly $500,000, according to a spokesman. Source: http://www.thecorsaironline.com/news/cctv-cameras-on-campus-are-catching-crime-1.2042123

DHS to gain real-time access to DoD biometrics. The Department of Homeland Security (DHS) hopes to soon have real-time access to the military's biometrics database letting them better sort out who's who at U.S. points of entry. The capability will be similar to what DHS is already doing with the FBI, and through it, local law enforcement agencies around the country said the director of DHS's U.S. VISIT program. U.S. VISIT, the office responsible for screening foreign visitors to the U.S.-is the main repository for DHS' biometric data. That information, mainly fingerprint data, can be shared between DHS and the criminal record system that the FBI holds at its Criminal Justice Information Services division in West Virginia. The director said DHS had already proven the value of biometric information sharing through the Secure Communities program, which lets participating local law enforcement see data held in Homeland Security databases. He said that data comes in handy when law officers encounter a suspect who gives a false name. Since DHS also has access to biometric data held by the FBI, its Customs and Border Protection agents can make better decisions about who to let into the country. "Prior to a pilot in Detroit that we will now expand to other locations, we had people coming into the country with criminal history that made them ineligible to come into the country," the director said. "But they came into the country because we didn't know about it. We can now search the FBI's criminal master file-65 million prints-in under 15 seconds. That is a tremendous, tremendous step forward in both the idea of leveraging information sharing and the technical interoperability between the two systems." Source: http://www.federalnewsradio.com/?nid=35&sid=2289626

Immigration officials: Tri-Valley U. and students involved in Visa scam. Tri-Valley University (TVU) in Pleasanton, California is being investigated by federal officials who suspect it made millions of dollars by luring hundreds of foreign students to enroll by promising to take care of their Visa problems. Investigators also believe many TVU students shared in the possible fraud by collecting a share of the tuition of other students they recruited to the school. "Once enrolled at TVU, each foreign national may also collect up to 5 percent of the tuition of any new student that his or her referred student refers. A large percentage of foreign nationals at TVU participate in this referral/profit-sharing statement," court documents alleged TVU was shut down January 19 and labeled a "sham university"

by immigration officials. When the school was shut down, more than 1,000 foreign students were stripped of their student status that allows them to stay in America to study. Since January, at least 18 students were required by Immigration and Customs Enforcement to wear ankle bracelets so their locations could be tracked. Source: http://abcnews.go.com/US/immigration-officials-tri-valley-university-sham-selling-student/story?id=12974636

U.S. Embassy in Libya closed, Americans evacuated. The U.S. State Department announced February 25 that it had closed the U.S. Embassy in Libya in response to increasing violence there. According to a White House spokesman, a ferry with about 200 U.S. citizens arrived safely in Malta. "The State Department has suspended embassy operations in Libya and will temporarily withdraw all embassy employees from Tripoli," the spokesman said. Remaining embassy personnel and American citizens who requested evacuation were flown via charter plane to Istanbul, Turkey. Other nations from Britain to China were also scrambling to get their citizens out of the country as Libya's leader struggled to hold on to his slipping grip on power. Source: http://www.wistv.com/Global/story.asp?S=14143715

(Iowa) **More students arrested in Storm Lake school bomb threats.** Eight students were arrested in a series of bomb threats at Storm Lake Middle School in Storm Lake, Iowa. The students, ranging in age from 11 to 16, were arrested after written notes containing the threats were found in the school February 24 and 25. The school was evacuated because of the three rounds of threats. A school board member said each threat has to be treated seriously even if officials suspect a prank or copycat. He said the students do not understand how much damage they did. The students face various charges, including terroristic threat and harassment. Some were released by police to their parents; others were placed in a juvenile detention center. Source: http://www.kgan.com/shared/newsroom/top_stories/videos/kgan_vid_5103.shtml

Information Technology and Telecommunications

Twitter crime rate rises 20 percent. Barracuda Labs analyzed more than 26 million Twitter accounts in order to measure and analyze account behavior. The analysis enabled researchers to model normal user behavior and identify features that are strong indicators of illegitimate account use. Key highlights from the Twitter research include: In general, activity continues to increase on Twitter: more users are coming online; true Twitter users are tweeting more often, and even casual users are becoming more active. As users become more active, the malicious activity also increases. The number of real Twitter users increased to 43 percent, up from only 29 percent in June 2010. For every 100 Twitter users, 39 have between 1 and 9 followers, while 50 percent of Twitter users have more than 10 followers. Approximately 79 percent of Twitter users tweet less than once per day. After decreasing at the end of 2009, the Twitter crime rate increased 20 percent from the first half of 2010 to the second half of 2010, going from 1.6 percent to 2 percent. Attackers are distributing malware and exploiting vulnerabilities to achieve their malicious goals. Source: http://www.net-security.org/malware_news.php?id=1652

iTunes 10.2 addresses multiple security vulnerabilities. Apple has released an update, version 10.2, to the popular iTunes media player software, closing a number of security vulnerabilities in its product. According to Apple, iTunes 10.2 corrects five vulnerabilities in ImageIO, as well as two issues

in the libxml library, many of which could possibly be used by an attacker to execute arbitrary code. The update also fixes a total of 50 bugs in the WebKit browser engine which could also lead to arbitrary code execution via a man-in-the-middle attack while browsing the iTunes Store. Source: http://www.h-online.com/security/news/item/iTunes-10-2-addresses-multiple-security-vulnerabilities-1201288.html

Rootcager trojan found on the official Android market. Free Android applications bundled up with malware have spilled over into the official Android marketplace. According to Symantec, the malware in question can root the phone, harvest data and open backdoors — similar to the recent Geimini Trojan spotted lurking on third-party Chinese Android app markets. "The applications in question are popular free apps, bundled with malware, that have then been republished in the official marketplace under different application and publisher names," said a researcher. Google has removed the applications from the market, but according to Symantec's sources somewhere between 50,000 and 200,000 downloads took place during the 4 days that the apps were available for download. This new trojan has been dubbed Rootcager because of the rageagainstthecage file included in the Android Package containing the affected apps. Rageagainstthecage is a file that can also be used to legitimately root a phone in order for the users to gain administrative rights, but in this case it is used to allow the trojan to do things like taking screenshots, harvesting IMEI and IMSI numbers and send them to remote sites, and drop a DownloadProvidersManager Android Package that will further execute downloads in the background. Source: http://www.net-security.org/malware_news.php?id=1648

Infected Android app runs up big texting bills. A rogue Android application tweaked by hackers can hijack a smartphone and run up big texting bills before the owner knows it, Symantec said February 28. The newest in a line of compromised Android apps, said a principle security response manager at Symantec, is Steamy Window, a free program that Chinese hackers modified, then re-released into the wild. The cyber criminals grabbed a copy of Steamy Windows, then added a backdoor trojan horse — "Android(dot)Pjapps" by Symantec's label — to the app's code. The reworked app is placed on unsanctioned third-party "app stores" where unsuspecting or careless Android smartphones find it, download it, and install it. The trojan planted by the malware-infected Steamy Windows can install other applications, monkey with the phone's browser bookmarks, surreptitiously navigate to Web sites, and silently send text messages, said the Symantec response manager. The last is how the criminals make money. "The Trojan lets them send SMS [short message service] messages to premium rate numbers," he said, for which the hackers are paid commissions. Source: http://www.computerworld.com/s/article/9211879/Infected_Android_app_runs_up_big_texting_bills?taxonomyId=17

Popular Websites hit by malvertizing attack. Internet users were prompted by security alerts when browsing popular Web sites the weekend of February 26 and 27 because of a malvertizing campaign pushed exploits onto their pages. It is unclear where the attacks originated, but many reports seem to focus on a domain called stripli(dot)com from where the malicious advertisements were loaded. This domain is currently blacklisted by Google's Safe Browsing service, which means Web sites trying to load content from it could end up being blocked in Chrome and Firefox. The site in this case was www(dot)londonstockexchange(dot)com, and attempting to visit it from Google Search and these two browsers resulted in a Safe Browsing error. The diagnostic page for stripli(dot)com stated "this

site has hosted malicious software over the past 90 days. It infected 7 domain(s), including reviewcentre(dot)com, londonstockexchange(dot)com, viamichelin(dot)com/." But, according to reports on Yahoo! Answers, the impact was much more extensive, with IMDb(dot)com and eBay(dot)com being among the affected domain names. Google's Safe Browsing service did not have time to blacklist these domains until they resolved the problem, but some users were alerted by their antivirus programs about malicious code being served from them. On some forums people reported being infected with a fake antivirus program after browsing through the affected sites.Source: http://news.softpedia.com/news/Several-Popular-Websites-Hit-by-Malvertizing-Attack-186660.shtml

150,000 Gmail accounts reset and contents deleted. Word about the accidental resetting of G-mail accounts has been spreading on the Internet in the last 2 days as users Tweeted that their e-mail accounts were stripped clean of all e-mails, attachments, and chat logs collected in them over the years. Google confirmed the glitch and its results, saying that less than 0.08 percent (around 150,000) of the Google Mail user base has been affected. The issue has still not been resolved and some users still cannot access their accounts. Google confirmed "users may be temporarily unable to sign in while we repair their accounts", but did not say if the content would be restored. Source: http://www.net-security.org/secworld.php?id=10671

Hacker writes easy-to-use Mac Trojan. Researchers at Sophos said they have spotted a new trojan horse program written for the Mac. It is called the BlackHole remote access trojan, and it is easy to find online in hacking forums, a Sophos researcher said. Sophos has not seen the Trojan used in any online attacks — it is more a bare-bones, proof-of-concept beta program now — but the software is easy to use, and if a criminal could find a way to get a Mac user to install it, or write attack code that would silently install it on the Mac, it would give him remote control of the machine. BlackHole is a variant of a Windows Trojan called darkComet, but it seems to have been written by a different developer. The darkComet source code is freely available, so it appears BlackHole's author took it and tweaked it so it would run on the Mac, the researcher said. Source: http://www.computerworld.com/s/article/9211659/Hacker_writes_easy_to_use_Mac_Trojan

Spear phishing attacks leverage Libya crisis to deliver exploit. Security researchers from Symantec warned of highly targeted attacks that leverage the crisis in Libya to deliver an exploit via e-mail and infect computers. The e-mails pose as replies to previous messages about the current situation in the Arab country. Their body contains a very short message reading "I agree with this point," however, a formatting error results in a broken html tag to also appear at the end. The short message has the purpose of diverting recipients' attention towards the attached document called "EconomicStakes in Libya's Crisis(dot)doc." If opened, the document tries to exploit an Office RTF stack buffer overflow vulnerability, identified as CVE-2010-3333 and patched by Microsoft in November. Successful exploitation allows the attacker to execute arbitrary code on the system. In this case a piece of malware is installed. According to Symantec, the attacks intercepted by the company targeted 27 individuals within 6 different organizations involved in human rights activism, humanitarian aid, or the analysis of foreign affairs and economic development. Source: http://news.softpedia.com/news/Spear-Phishing-Attacks-Leverage-Libya-Crisis-to-Deliver-Malware-186441.shtml

National Monuments and Icons

(Texas) **About 120,000 acres burn in Texas wildfires.** About 120,000 acres have burned in West Texas as the wind eased and crews brought all of the fires under control. A spokesperson with the Texas Forest Service (TFS) said March 1 that firefighters were putting out hot spots at various locations. He said the high fire danger would continue throughout the week, but it was much improved since wildfires broke out February 27. Lighter winds February 28 helped with firefighting efforts. TFS responded to fires that blackened about 120,000 acres, but the number could go higher when volunteers file their reports on other blazes they fought. Aircraft assigned to firefighting duty were able to fly February 28, a day after being grounded during strong winds. Source: http://www.chron.com/disp/story.mpl/ap/tx/7450946.html

Postal and Shipping

DOT issues tougher hazmat shipping rule. The U.S. Department of Transportation's Pipeline and Hazardous Materials Safety Administration announced March 3 department inspectors will now have greater authority when it comes to ensuring the safety of hazardous materials in the stream of transportation. The new rule, which implements authority granted by Congress, allows inspectors to investigate shipments of hazardous materials during transport and take tougher enforcement action against companies shipping in an unsafe manner. The new authority allows department inspectors to close down shipping companies with poor safety records. It also specifically authorizes inspectors to take immediate action when there is a significant safety problem with a package in transit. This includes ordering restrictions, bans, or immediate recalls of faulty packages. With these new provisions, inspectors will be able to temporarily detain and inspect packages that may pose a serious threat to life, property, or the environment. Department inspectors will also be able to immediately open packages even if the request to open them is refused. Source: http://ohsonline.com/articles/2011/03/03/dot-issues-tougher-hazmat-shipping-rule.aspx?admgarea=news

Public Health

FDA orders 500 cough and cold drugs off the market. The U.S. Food and Drug Administration (FDA) March 2 ordered the makers of about 500 unapproved prescription cough and cold medicines to get them off the market because they have not been proven safe and effective. The drugs have been linked to a few relatively minor problems, such as drowsiness and irritability, but the FDA is concerned medical problems associated them may be significantly underreported. Some of the targeted drugs are labeled as suitable for infants and children but contain ingredients covered by a 2008 FDA advisory that warned against using over-the-counter medications in children under age 2. Others are billed as timed-release products. Such medications are difficult to manufacture and, if quality controls are inadequate, some may release drugs too slowly, too quickly or not at all. The FDA also moved against several unapproved products that contain possibly dangerous combinations of drugs, such as two antihistamines, which can cause oversedation. The FDA included Cardec, Lodrane 24D, Organidin, and Pediahist as brands consumers may have encountered. Many of the drugs came on the market before a 1962 law that required makers to prove their effectiveness. It is not clear how

much of a public health threat they may pose. Source: http://www.latimes.com/health/la-na-unapproved-drugs-20110303,0,4370223.story

(Illinois) **CDC details cause of 2009 plague death.** The University of Chicago scientist who died in 2009 while conducting vaccine research using a weakened strain of plague bacterium succumbed to his infection because of an underlying medical condition, Bloomberg reported last week. The enervated strain of Yersinia pestis the scientist worked with was thought to pose no health risk to humans. His 2009 death initially perplexed infectious disease experts as he was judged to have adhered to all the necessary safety rules. Specialists now believe he was especially susceptible to the plague due to his then-unrealized hemochromatosis, a medical disorder in which too much iron builds up in the body, according to a recently released report by the U.S. Centers For Disease Control and Prevention. The case demonstrates that regardless of the degree to which plague material is altered, there will be individuals who are susceptible to infection, a University of Chicago infectious disease specialist said. Source: http://gsn.nti.org/gsn/nw_20110301_2791.php

D.C. Health Department issues measles alert. A woman infected with measles traveled through Washington, D.C. and Maryland after flying into Dulles International Airport in Dulles, Virginia, it was disclosed February 28. The 27-year-old New Mexico resident landed at the airport February 20 and left the region February 22, from Baltimore-Washington International Marshall Airport (BWI) in Baltimore, Maryland. D.C. Health Department officials said she spent time in Washington, D.C. during this period, apparently in Georgetown and Columbia Heights. The department said between 10:30 a.m. and 2:30 p.m. February 21, the woman went from Georgetown to Columbia Heights, using buses on the D1 or D6 route for part of the trip. She apparently returned between 1:30 p.m. and 5:30 p.m. on an S2 or S4 bus, the health department said. In Columbia Heights, she might have been at the Potbelly Sandwich Shop in the 1400 block of Irving Street NW. The medical director of the public health division of the New Mexico Health Department said the woman apparently was exposed to measles while in Europe. She flew from BWI to Denver, and then to Albuquerque. Source: http://www.washingtonpost.com/wp-dyn/content/article/2011/02/28/AR2011022806618.html?hpid=newswell

Air travelers may have been exposed to measles. Public health officials are warning travelers and workers present at four U.S. airports on two recent days that they may have been exposed to measles from a traveler arriving from London, England. Authorities said February 26 that a New Mexico woman later confirmed to have measles arrived at Washington Dulles International Airport in Dulles, Virginia late in the afternoon of Feb. 20. Two days later, the measles-infected traveler departed from BWI Thurgood Marshall Airport near Baltimore, Maryland on an evening flight to Denver, Colorado, and then on to Albuquerque, New Mexico. The traveler became sick and was subsequently diagnosed with measles in New Mexico, a spokesman for the Centers for Disease Control and Prevention (CDC) said. He said February 26 that authorities in those states are trying to notify travelers who sat close to the infected passenger on the flights. The New Mexico Department of Health's scientific laboratory division said the traveler was a 27-year-old Santa Fe woman who had not been immunized against measles. "The appropriate steps are being taken to reach out to those passengers on the plane that were in close enough proximity," the CDC spokesman said of those seated five rows in front or behind the infected passenger. Although most Americans have been vaccinated for measles or are immune because they've had the disease, public health officials are

concerned about those not immunized, including babies. Pregnant women and those with weakened immune systems are also more at risk. Authorities say people who were at the airports at the same time as the infected traveler and develop a fever or other symptoms should contact their doctors. An infectious disease specialist at the Vanderbilt University School of Medicine in Nashville said the potential exposure of so many travelers in airport terminals is a cause for concern. He said measles is "highly communicable" and can be associated with complications leading to death. "We don't want measles to be imported back into the U.S. once it gets a foothold." Source: http://www.cbsnews.com/stories/2011/02/28/travel/main20037210.shtml

Transportation

Bill to criminalize laser pranks advances. People who knowingly aim laser pointers at aircraft — which can distract or temporarily blind pilots — would be committing a federal crime subject to up to 5 years in prison under a measure passed by the U.S. House of Representatives February 28. The Senate approved the measure 1 month ago. The two chambers must now decide whether to send it to the President as separate legislation or an amendment to another bill. The Federal Aviation Administration said 2,836 people pointed lasers at planes and helicopters in 2010. Source: http://www.nytimes.com/2011/03/01/us/01brfs-BILLTOCRIMIN_BRF.html?_r=1

Final rule targets texting for intrastate hazmat haulers. A ban on texting while driving a commercial vehicle has been in effect since September 2010. A new final rule issued February 28 by federal regulators casts the net wider to include hazmat haulers that do not cross state lines. The Pipeline and Hazardous Materials Safety Administration (PHMSA) issued a final rule February 28, to prohibit texting while driving a commercial vehicle hauling hazardous materials. The rule takes effect March 30, according to the Federal Register announcement. The PHMSA rule expands on the Federal Motor Carrier Safety Administration's (FMCSA) final rule for interstate commercial drivers. The agencies cite the same studies, one by Virginia Tech in particular, to justify the regulatory actions. Source: http://www.landlinemag.com/todays_news/Daily/2011/Mar11/030411/030111-02.shtml

Threat made against US-bound flights from Jamaica. Jamaican authorities said cargo flights to the United States were temporarily suspended due to a reported threat. A U.S. Transportation Security Administration spokesman said March 1 that the agency is helping the Jamaicans with "precautionary security measures" for U.S.-bound flights following what he called "unsubstantiated threat information." He said it is being done out of "an abundance of caution." Jamaica's civil aviation authority says a temporary suspension of air cargo and duty free items to the U.S. was imposed February 27 evening after an "unconfirmed report" of a threat. U.S. and Jamaican officials refused to disclose specifics about the threat or say when flights will resume. Source: http://www.businessweek.com/ap/financialnews/D9LMM3RO0.htm

Water and Dams

Nothing Significant to Report

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**